Deutsches Patent- und Markenamt DEPATISnet

Bibliographische Daten Dokument US000006775398B1 (Seiten: 7)

	Feld	Inhalt
Titel	TI	[ ] Method and device for the user-controlled authorisation of chip-card functions
Anmelder	PA	INTERNATIONAL BUSINESS MACHINES CORPORATION
Erfinder	IN	SCHAECK THOMAS ; WALZ THOMAS
Anmeldedatum	AD	27.12.1999
Anmeldenummer	AN	472452
Anmeldeland	AC	US
Veröffentlichungsdatum	PUB	10.08.2004
Prioritätsdaten	PRC PRN PRD	DE 19860177 19981224
IPC-Hauptklasse	ICM	G06K 9/00
IPC-Nebenklasse	ICS	
IPC-Doppelstrichklasse	ICA	
IPC-Indexklasse	ICI	
Abstract	AB	[ ] The present invention describes a device and a procedure for the user-controlled release of chip-card functions in particular through the input of authentication data. The input of the authentication data takes place by way of an input device of a mobile chip-card reader, particularly one designed as a pocket chip-card reader. The authentication data are checked in the chip-card on the basis of a reference list. If the authentication data agree with the reference-data, a function stored in the non-volatile memory of the chip-card is released. The released function can be specified by number, time and period of validity. The chip-card can then be used in a terminal in accordance with the specified release. The present invention thereby guarantees in a simple manner, that authentication data cannot leave the area under the control of the user's chip-card. Moreover, the authentication ensures that only functions released by the authorization such as, for example, the production of a signature or read or write commands, are executed.

Zurück zur Trefferliste | Drucken | PDF-Anzeige | Schließen

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 60 177 A 1**

(51) Int. Cl.[7]:
G 06 F 3/08
G 06 F 17/60
G 07 C 9/00

(21) Aktenzeichen: 198 60 177.8
(22) Anmeldetag: 24. 12. 1998
(43) Offenlegungstag: 6. 7. 2000

(71) Anmelder:
International Business Machines Corp., Armonk, N.Y., US

(74) Vertreter:
Teufel, F., Dipl.-Phys., Pat.-Anw., 70569 Stuttgart

(72) Erfinder:
Walz, Thomas, 75223 Niefern-Öschelbronn, DE;
Schaeck, Thomas, 77855 Achern, DE

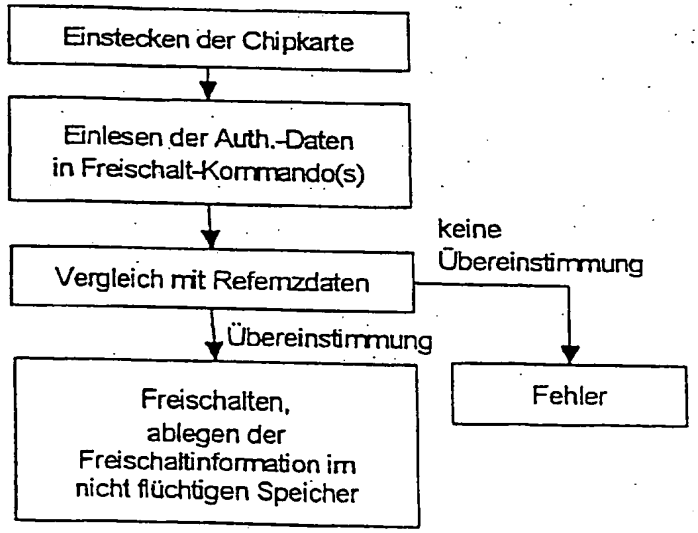
(56) Entgegenhaltungen:
DE 37 06 466 C2
EP 02 91 834 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und Vorrichtung zur benutzerkontrollierten Freischaltung von Chipkartenfunktionen

(57) Die vorliegende Erfindung beschreibt eine Vorrichtung und ein Verfahren zum benutzerkontrollierten Freischalten von Chipkartenfunktionen insbesondere durch die Eingabe von Authentisierungsdaten.
Die Eingabe der Authentisierungsdaten erfolgt über eine Eingabevorrichtung eines mobilen Chipkartenlesegeräts, die insbesondere als Taschenchipkartenleser ausgebildet ist. Die Authentisierungsdaten werden in der Chipkarte anhand einer Referenzliste überprüft. Bei Übereinstimmung der Authentisierungsdaten mit den Referenzdaten wird im nichtflüchtigen Speicher der Chipkarte eine dort abgelegte Funktion freigeschaltet. Die freigeschaltete Funktion kann nach Anzahl, Zeitpunkt und Gültigkeitsdauer spezifiziert sein. Die Chipkarte kann dann in einem Terminal entsprechend der spezifizierten Freischaltung verwendet werden. Die vorliegende Erfindung stellt damit auf einfache Weise sicher, dass Authentisierungsdaten den Kontrollbereich des Benutzers der Chipkarte nicht verlassen können. Darüber hinaus wird durch die Authentisierung sichergestellt, dass nur vom Authentisierten freigeschaltete Funktionen, wie z. B. Erstellen einer Signatur oder Lese- oder Schreibbefehle, ausgeführt werden.



DE 198 60 177 A 1

DE 198 60 177 A 1

Beschreibung

Die vorliegende Erfindung beschreibt ein Verfahren und eine Vorrichtung zur benutzerkontrollierten Freischaltung von Chipkartenfunktionen.

Die Freischaltung bzw. die Ausführung von bestimmten Chipkartenfunktionen setzt in vielen Fällen die Authentisierung des Kommunikationspartners voraus. Für die Chipkarte bedeutet dies, dass die Chipkarte feststellen muß, ob der Benutzer der Chipkarte oder das Terminal berechtigte Kommunikationsspartner sind.

Dies wird im Regelfall dadurch sichergestellt, dass die Kommunikationspartner ein gemeinsames Geheimnis besitzen, das mit Hilfe eine Authentisierungsverfahrens überprüft wird.

Bei heutigen Systemen zur Benutzer-Authentifikation, z. B. Zugangsberechtigungen zu Gebäuden, Transaktionsauthentifikationen bei Bankgeschäften (Bankomat, Home-Banking, Telefonbanking) Handy etc., wird dem Benutzer ein Geheimnis übergeben, mit welchem er sich als der authentischer Benutzer identifiziert. Im Regelfall erfolgt dies durch die Ausgabe eines PINs oder Paßwortes.

Diese geheime Information wird von der autorisierenden Einheit (Geldautomat, Hostrechner, PC, Internet usw.) verifiziert. Bei der Überprüfung ergibt sich folgende Problemstellung:
das Geheimnis soll keiner fremden Person zugänglich sein, d. h. das Geheimnis muß zwischen Eingabe und Überprüfungsstelle bestmöglichst geschützt werden,
alle auf dem Übertragungsweg eingesetzten Komponenten müssen als Einzelkomponenten denselben Sicherheitsstandard Genüge leisten.

Der PIN wird, z. B. bei Geldautomaten, vor Ort in derselben physikalischen Einheit "Encrypting PIN Pad" bereits verschlüsselt, um diese vor unberechtigten Zugriffen zu schützen. Dies soll einen Angriffsversuch auf den PIN an der PIN-Tastatur und den nachfolgenden Kommunikationskomponenten verhindern. Der Besitz dieser geheimen Information eröffnet einem Angreifer die Möglichkeit einer unberechtigten Authentifikation, da dieses Geheimnis portabel ist.

Vor diesem Hintergrund gibt es verstärkt Bestrebungen, biometrische Informationen zur Benutzerauthentifikation einzusetzen. Zu nennen sind hier Fingerabdruck, Netzhauterkennung oder Gesichtserkennung. Diese Systeme bieten den Vorteil, daß zur Authentifikation ein Körpermerkmal des Benutzers benutzt wird, welches mit hoher Wahrscheinlichkeit nur einem Benutzer zugeordnet werden kann und daher nicht übertragbar ist. Diese "Nichtübertragbarkeit" und Eindeutigkeit" bietet den Vorteil, dass sich der Kunde das Geheimnis nicht merken muß und das Geheimnis nicht entwendet werden kann.

Ein wesentlicher Nachteil der biometrischen Authentisierungsverfahren liegt darin, das biometrische Werte zur Authentisierung nicht beliebig verfügbar sind. Wird in einem System der PIN ausgespäht ("variables Geheimnis"), kann ein neuer PIN festgelegt werden, wodurch der alte PIN unbrauchbar wird.

Ist ein biometrischer Wert, z. B. Fingerabdruck, einem Angreifer zugänglich geworden, so besteht die Möglichkeit einen neuen Fingerabdruck auszuwählen, wodurch der frühere Fingerabdruck unbrauchbar wird. Das biometrische Authentisierungsverfahren läßt sich in diesem Fall maximal zehnmal wiederholen bis die biometrische Fingerabdruckwerte eines Menschen erschöpft sind.

Deshalb ist es sehr gefährlich, Systeme mit biometrischen Eingabesystemen in Einsatz zu bringen, sofern diese Systeme nicht einen sehr hohen Sicherheitsstandard erfüllen.

Die derzeit bekannten Sicherheitssysteme lassen sich in folgende Komponenten zerlegen:

1. Eingabemedium zur Eingabe des Authentisierungswertes
2. Übertragungsmedium zur Übermittlung des Authentisierungswertes
3. Überprüfungsstelle zur Überprüfung der Richtigkeit des Authentisierungswertes

Der Authentisierungswert, z. B. PIN, wird mittels einer numerischen Tastatur eingegeben und über das Netzwerk a. einen Hostrechner weitergegeben. Im Hostrechner erfolgt der Vergleich des eingegebenen PINs mit dem Referenz PIN.

Eine andere Ausführungsform kann darin bestehen, das anstatt der Eingabe eines PINs eine biometrische Eingabe erfolgt. Hier kommt insbesondere ein Fingerabdrucksensor in Betracht, der die Fingerabdruckdaten über ein Netzwerk zu einem Hostrechner weiterleitet, wo schließlich eine Vergleichsprüfung erfolgt.

Der Schutz des Übertragungsweges läßt sich in verteilten Systemen durch technische Maßnahmen realisieren. Es besteht aber immer die Möglichkeit, daß eine Komponente im Gesamtsystem manipuliert ist bzw. wird.

So könnte z. B. zwischen Fingerabdrucksensor und Hostsystem der Wert "mitgehört" werden und zu einem späteren Zeitpunkt für eine nicht legale Transaktion eingespielt werden.

– Die Gesamtzahl der Komponenten eines Systems können von einem Benutzer unmöglich übersehen werden.

Es ist daher Aufgabe der vorliegenden Erfindung, eine Vorrichtung und ein Verfahren bereitzustellen, das die Überprüfung der Authentität eines Benutzers zur Ausführung von Chipkartenfunktionen auf einfache und sichere Weise unabhängig von dem jeweiligen Authentisierungsverfahren sicherstellt.

Diese Aufgabe wird durch die Merkmale des Anspruchs 1 und 10 gelöst. Weitere vorteilhafte Ausführungsformen sind in den Unteransprüchen niedergelegt.

Die Vorteile der vorliegenden Erfindung liegen darin, dass der erfinderische Taschenchipkartenleser zur Freischaltung von Chipkartenfunktionen sich im ausschließlichen Kontrollbereich des Berechtigten befindet. Manipulationen am Taschenchipkartenleser, insbesondere das unberechtigte Freischalten von schützenswerten Funktionen, lassen sich daher durch den Berechtigten weitgehend ausschließen. Dies gilt insbesondere bei der Eingabe eines PINs oder einer biometrischen Eingabe. Die Überprüfung der Richtigkeit des eingegebenen Pins erfolgt in der Chipkarte, über den der Berechtigte ebenfalls die ausschließliche Verfügungsgewalt hat. Der PIN verläßt daher nicht den Kontrollbereich des Berechtigten, wodurch ein Mißbrauch bzw. Ausspähen des PINs oder des biometrischen Wertes durch unberechtigte Dritte ausgeschlossen ist. Der erfinderische Taschenchipkartenleser kann sowohl mit einer numerischen als auch einer biometrischen Eingabevorrichtung versehen werden. Die Authentifizierung des Berechtigten führt zur Freischaltung der Chip-

karte für bestimmte Transaktionen, die entweder zeitlich oder anzahlmäßig limitiert werden können. Dies schützt die freigeschaltete Chipkarte gegen dauernden Mißbrauch durch Dritte.

Die vorliegende Erfindung wird anhand mehrerer Ausführungsbeispiele anhand Figuren näher beschrieben, wobei

Fig. 1 den erfinderischen Taschenchipkartenleser mit seinen Komponenten zeigt

Fig. 2 ein Ablaufdiagramm des erfinderischen Taschenchipkartenlesers nach **Fig.** 1 zeigt

Fig. 3 ein Ablaufdiagramm für die nach **Fig.** 2 freigeschaltete Chipkarte in einem Terminal zeigt

Fig. 4 eine indirekte biometrische Authentisierung unter Verwendung des erfinderischen Taschenchipkartenlesers nach **Fig.** 1

Im nachfolgenden wird der erfinderische Taschenchipkartenleser anhand **Fig.** 1 beschrieben. Der Taschenchipkartenleser **1** besteht vorzugsweise aus Gehäuse mit Schalter, Batterie und Mikroprozessor. Bei dem Gehäuse handelt es sich vorzugsweise um ein Kunstoffgehäuse im Format einer DIN Kreditkarte. Im Gehäuse befindet sich ein Mikroschalter, welcher bei vollständig eingeführter Chipkarte **5** einen Mikroprozessor mit der Batterie verbindet, wodurch dieser sein Programm startet.

Zwischen Mikroprozessor und Chip auf der Chipkarte **5** wird über die Chipkartenkontaktierstation **2** kommuniziert.

Über die Anzeige **3**, die vorzugsweise als LCD-Anzeige ausgestaltet ist, wird der Benutzer geführt. Nach Einführen der Chipkarte wird er zur Eingabe seiner Authentifikationdsaten aufgefordert, z. B. "PIN eingeben" oder "Finger auf Sensor drücken".

Der Fingerabdrucksensor **4** nimmt die Vergleichsdaten des Kunden auf und übermittelt diese über die Signalleitung **6** zu dem Mikroprozessor. Als Fingerabdrucksensor kommen "statische" oder "dynamische" Sensoren zum Einsatz. Statischer Einsatz bedeutet, dass der Kunde seinen Finger auf den Sensor drückt, welcher somit, auf einmal die ganze Fläche der Fingerkuppe erfassen muß.

Dynamischer Einsatz bedeutet, dass der Kunde seinen Finger über einen schmalen Sensor bewegen (ziehen) muß. Der Sensor kann kleiner implementiert werden, da er nur in der Breite die Größe der Fingerkuppe erfassen muß.

Mit dem derzeitigen Stand der Technik ist es möglich, einen Fingerabdrucksensor auf Halbleiterbasis mit den Maßen kleiner 20 × 20 mm herzustellen. Statische Sensoren verdienen von der Kundenhandhabung und vom Platzbedarf den Vorzug.

Auch die Integration einer numerischen Tastatur in den erfinderischen Taschen-Chipkartenleser ist technisch ebenfalls unproblematisch.

Die Fingerabdruck-/PIN-Daten gehen unmittelbar zur Chipkarte – ohne hierbei jedoch das System zu verlassen – und werden dort mit den sicher gespeicherten Referenzdaten verglichen.

Der Kunde kann mit dem in seinem Besitz befindlichen Taschenchipkartenleser eine Authentisierung veranlassen.

Nach Eingabe und Überprüfung des Fingerabdruckes oder des PINs in der Chipkarte wird die Chipkarte für eine vordefinierte Anzahl von Kommandos freigeschaltet. Freischalten von Kommandos bedeutet das Ändern des Zustands einer Chipkarte derart, dass nach der Zustandsänderung bestimmte Funktionen der Karte für bestimmte Zeit, bestimmte Häufigkeit der Ausführung oder unbegrenzt ausgeführt werden können. Das Freischalten ist somit eine Zugriffsvoraussetzung für das Ausführen einer Chipkartenfunktion. Mit einem Objekt (z. B. einem kryptographischen Schlüssel) auf einer Chipkarte und einer Gruppe von Kommandos (zum Beispiel dem Kommando zum Erzeugen einer digitalen Signatur) assoziierte Bedingung, die vor dem Ausführen eines Kommandos dieser Gruppe gegen das Objekt erfüllt werden muss. Eine solche Bedingung ist z. B. das erfolgreiche Durchführen einer Authentisierung des Karteninhabers. Die freigeschaltete Chipkarte kann in einem Kunden Terminal verwendet werden. Dies geschieht wie folgt: die Chipkarte wird in das Terminal eingeführt (Kartenleser). Eine Transaktion wird ausgewählt.

Das Terminal nimmt mit der Chipkarte Verbindung auf. Ist die Karte für eine oder mehrere Transaktion(en) freigeschaltet so wird diese initiiert; ist dies nicht der Fall, muß der Authentifikationswert am Terminal (z. B. PIN) eingegeben werden.

Falls die Chipkarte freigeschaltet in falsche Hände gerät, kann sie maximal für die Anzahl der freigeschalteten Transaktionen verwendet werden (normalerweise werden 1–2 Transaktionen freigeschaltet).

Eine weiterer Schutz bietet hier die "Zeit limitierte Freischaltung einer Transaktion". Dies bedeutet, daß die Chipkarte sich wieder für Transaktionen sperrt falls keine Transaktionen in einem vordefinierten Zeitraum nach der Freischaltung erfolgt sind. Chipkartenanwendungen sind z. B. Geldkarte am Bankautomat, Internetbanking, Homebanking, Bankomat, Zugangsberechtigung, Handy Aktivierung, Krankenkasse, Tankstellen, Kreditkarte, Datenzugriff, Workstationzugang und Laptop Zugriff.

Würden die in der Chipkarte abgelegten Referenzdaten ausgespäht werden, so muß dies pro Chipkarte, d. h. pro Runde mit dessen Chipkarte erfolgen. Die in verteilten Systemen bestehende Möglichkeit der Aufzeichnung von Referenzdaten einer Vielzahl von Kunden ist daher ausgeschlossen.

Die Benutzerakzeptanz dieses Systems kann als sehr hoch eingeschätzt werden, da der Kunde das Authorisierungssystem, z. B. PC im InternetCafe, POS Station in der Tankstelle etc. nicht mehr komplett überblicken muß.

Der Benutzer der vorliegenden Erfindung ist jedoch in der Lage seine Authentisierungs-Hardware voll zu überblicken. Deshalb bietet der erfinderische Taschenchipkartenleser einen größtmöglichen Schutz vor Mißbrauch, da sich alle Komponenten im ausschließlichen Kontrollbereich des Benutzers befinden.

Die PIN oder die biometrischen Authentifikationdsaten gelangen daher ohne Wissen des Berechtigten nicht außerhalb des erfinderischen Taschenchipkartenlesers. Vergleichswerte, z. B. PIN oder Fingerabdruck, sind in einer sicheren Umgebung (Chipkarte) gespeichert. Implementierung als Kombination aus Taschenchipkartenleser mit Fingerabdrucksensor oder mit Numerischer Tastatur sind in einem kostengünstigem und heute schon realisierbarem Umfeld möglich.

Fig. 2 zeigt in Form eines Ablaufdiagramms die Funktionsweise des erfinderischen Taschenchipkartenlesers.

Eine Chipkarte wird im Taschenchipkartenleser des Karteninhabers freigeschaltet, um anschliessend in einem Terminal verwendet zu werden. Bei einem Taschenchipkartenleser mit Fingerabdrucksensor kann dies wie folgt implementiert werden: Die Chipkarte wird in den Leser mit Fingerabdrucksensor gesteckt. Die Fingerabdruckcharakteristika werden durch eine Sequenz von Kommandos in den Chip der Chipkarte übertragen. Es kann sich dabei um den digitalisierten

Fingerabdruck selbst oder um eine bereits für den Vergleich aufbereitete Darstellung, z. B. ein für den Abdruck charakteristisches Feld von Vektoren, handeln. In der Chipkarte werden nun die eingehenden Daten mit Referenzdaten verglichen, die in einem dafür vorgesehenen Datenbereich (z. B. eine Datei bei einer Dateiorientierten Chipkarte oder ein Applet-Attribut bei einer JavaCard) abgelegt sind.

Stimmt der Fingerabdruck mit den Referenzdaten überein, wird in einem nichtflüchtigen Datenbereich der Chipkarte die Information abgelegt, dass eine Überprüfung erfolgreich durchgeführt wurde. Dies ist erforderlich, damit die Information nicht verloren geht, wenn die Karte aus dem Taschenchipkartenleser mit Fingerabdrucksensor entnommen und in ein Terminal (z. B. Geldausgabegerät) gesteckt wird, in dem die freigeschaltete Funktion benutzt werden soll.

Das Chipkartenbetriebssystem ist so ausgeführt, dass es bei der Prüfung der Zugriffsbedingungen vor der Ausführung eines Kartenkommandos ggf. vorangegangene Freischaltungen berücksicht, die zuvor im nichtflüchtigen Speicher abgelegt wurden. Diese Information kann etwa als Tabelle abgelegt sein, deren Einträge z. B. Tupel der Form
<Zugriffsbedingung, Funktion, max. Anzahl der Ausführungen, Zeitpunkt, Dauer, . . .>
sein können.

Im folgenden wird der Ablauf des Freischaltens im erfinderischen Taschenkartenleser anhand einer konkreten Implementierung dargestellt:

1. Die Daten zur Authentisierung des Karteninhabers (Fingerabdruck, PIN, Retina-Scan, etc.) werden eingelesen.
2. Die eingelesenen Daten werden mit Referenzdaten im nicht flüchtigen Speicher der Karte verglichen.
3. Bei Übereinstimmung wird im nichtflüchtigen Speicher der Karte folgende Information abgelegt: Zugriffsbedingung (Authentisierung des Karteninhabers), freigeschaltete Kommandos (Signaturerzeugung), Anzahl erlaubter Ausführungen, Zeitpunkt der Freischaltung und Gültigkeitsdauer der Freischaltung.

Diese Informationen können z. B. in einem zyklischen File mit mehreren Records abgelegt werden, wobei neue Freischaltinformationen stets die jeweils ältesten überschreiben. Dieses zyklische File darf nicht lesbar sein, es darf nur vor. Kartenbetriebssystem selbst lesbar und beschreibbar sein.

Zugriffsbedingung	Freigeschaltete Kommandos	Anzahl erlaubter Ausführungen	Zeitpunkt der Freischaltung	Dauer
Zugriffsbedingung	Freigeschaltete Kommandos	Anzahl erlaubter Ausführungen	Zeitpunkt der Freischaltung	Dauer
Zugriffsbedingung	Freigeschaltete Kommandos	Anzahl erlaubter Ausführungen	Zeitpunkt der Freischaltung	Dauer
Zugriffsbedingung	Freigeschaltete Kommandos	Anzahl erlaubter Ausführungen	Zeitpunkt der Freischaltung	Dauer

Jede Zeile der abgebildeten Tabelle entspricht einem Record im zyklischen File. Beispielsweise können die Zugriffsbedingungen in einem Byte codiert werden, die freigeschalteten Kommandos durch jeweils ein Byte, die Anzahl der Ausführungen durch ein Byte, der Zeitpunkt der Freischaltung durch 6 Bytes und die Freischalt-Dauer in Minuten durch zwei Bytes.

Hier ein konkretes Beispiel:

Auth. des Karteninhabers	Erzeugen einer Digitalen Signatur	1 mal	18:39:00 12/08/98	10 min
Authentisierung des Terminals	Lesen	3 mal	18:39:01 12/08/98	10 min
Auth. des Karteninhabers	Lesen	1 mal	18:39:02 12/08/98	5 min
Auth. des Terminals	Schreiben	1 mal	18:39:03 12/08/98	5 min

Fig. 3 zeigt in Form eines Ablaufdiagramms die Funktionsweise einer freigeschalteten Chipkarte in einem Terminal:

1. Die Karte empfängt von einer Anwendung ein Signaturkommando, das die Nummer des zu verwendenden Schlüssels enthält.
2. Die Karte ermittelt die Zugriffsbedingungen, die zur Erzeugung einer digitalen Signatur mit diesem Schlüssel erforderlich sind.
3. Die Karte prüft, ob diese Zugriffsbedingungen erfüllt sind. Erfordern die Zugriffsbedingungen für den zu verwendenden Schlüssel, wie in diesem Beispiel eine Authentisierung des Karteninhabers, so prüft die Karte anhand ihres im flüchtigen Speicher repräsentierten Zustands, ob bereits eine Authentisierung durchgeführt wurde.
4. Wenn die Zugriffsbedingungen erfüllt sind, hier die Authentisierung des Karteninhabers, erzeugt die Karte eine

digitale Signatur, ansonsten fährt sie mit Schritt 5 fort.
5. Die Karte prüft durch Lesen des relevanten Bereichs im nicht flüchtigen Speicher, ob eine noch gültige Freischaltinformation für die erforderliche Zugriffsbedingung und die Signaturfunktion vorhanden ist.
6. Ist gültige Freischaltinformation für die Zugriffsbedingung (hier Auth. des Karteninhabers) und das Kartenkommando (hier Erzeugen einer Signatur) vorhanden, wird die Anzahl erlaubter Ausführungen in der Freischaltungsinformation für das Kommando um eins erniedrigt und das Kommando ausgeführt, andernfalls schickt die Karte einen Fehlercode zurück an die Anwendung.

Fig. 4 zeigt eine indirekte biometrische Authentisierung unter Verwendung des erfinderischen Taschenchipkartenlesers nach **Fig.** 1.

Man authentisiert sich nicht direkt durch Übertragung biometrischer Daten (z. B. Fingerabdruck, Retina-Scan) sondern durch indirekte biometrische Authentisierung. Das heisst, man authentisiert sich durch biometrische Eigenschaften gegenüber der Karte, woraufhin die Karte eine digitale Signatur erzeugt, die zur Authentisierung gegen den Server dient.

Die Karte erzeugt nur Signaturen, wenn zuvor eine biometrische Authentisierung des Inhabers gegen die Karte erfolgte. Der Vorteil dabei ist, dass biometrische Daten niemals übertragen werden und keine biometrischen Referenzdaten auf dem Server abgespeichert sein müssen. Bei der digitalen Signatur kann es sich z. B. um eine RSA- oder DSA-Signatur handeln.

Beispiel: Authentisierung gegen einen Company-Web-Server im Internet.

1. Die lokale Anwendung scannt mit Hilfe eines Fingerprint-Scanners den Fingerabdruck des Benutzers.
2. Die lokale Anwendung übergibt der Chipkarte den Fingerabdruck in einer geeigneten Darstellung.
3. Die Chipkarte überprüft den Fingerabdruck. Nach erfolgreicher Überprüfung lässt sie die Erzeugung von digitalen Signaturen mit Hilfe eines privaten Schlüssels auf der Karte zu.
4. Die Anwendung erzeugt mit Hilfe der Chipkarte eine digitale Signatur über eine von Server gesandte zufällige Bytefolge und sendet das Resultat zur Authentisierung zum Server.

Während des gesamten Vorgangs verlässt der Referenz-Fingerabdruck nie die Karte.

Patentansprüche

1. Vorrichtung zum Freischalten von Chipkartenfunktionen enthaltend zumindest:
   a) ein tragbares Gerät zur Aufnahme und Kontaktierung einer Chipkarte
   b) eine Eingabevorrichtung zur Eingabe von Authentisierungsdaten
   c) eine Chipkarte enthaltend eine oder mehrere Funktionen, die einer Freischaltung zur Ausführung bedürfen
   d) eine Überprüfungs- und Freischaltungskomponente zur Feststellung der Richtigkeit der Authentisierungsdaten und Freischaltung zumindest einer Funktion nach Überprüfung der Richtigkeit der Authentisierungsdaten, wobei die Überprüfungs- und Freischaltungskomponente in der Chipkarte installiert ist.
2. Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, dass das Gerät nach a) als Taschenchipkartenleser ausgebildet ist und zumindest aus einem Taschenchipkartenlesergehäuse, einer Energiequelle, einem Mikroprozessor, einem flüchtigen und einem nichtflüchtigen Speicher, einer Chipkartenkontaktierstation und einer Kommunikationskomponente zur Übermittlung der Authentisierungsdaten von der Eingabevorrichtung zur Chipkarte besteht.
3. Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Taschenchipkartenleser ein Display aufweist.
4. Vorrichtung nach Anspruch 1 bis 3, dadurch gekennzeichnet, dass die Eingabevorrichtung integriertes Teil des Taschenchipkartenlesers ist.
5. Vorrichtung nach Anspruch 1 oder 4, dadurch gekennzeichnet, dass die Eingabevorrichtung als numerische Tastatur oder biometrischer Fingerabdrucksensor ausgebildet ist.
6. Vorrichtung nach Anspruch 1 bis 5, dadurch gekennzeichnet, dass der biometrische Fingerabdrucksensor sowohl als statischer als auch dynamischer Sensor ausgebildet sein kann.
7. Vorrichtung nach Anspruch 1 bis 6, dadurch gekennzeichnet, dass im nichtflüchtigen Speicher der Chipkarte Referenzdaten abspeicherbar und dass diese Referenzdaten mittels der Überprüfungskomponente auf Übereinstimmung mit den eingegebenen Authentisierungsdaten überprüfbar sind.
8. Vorrichtung nach Anspruch 1 bis 7, dadurch gekennzeichnet, dass die im nichtflüchtigen Speicher der Chipkarte ablegbaren Funktionen mittels der Freischaltungskomponente innerhalb einer definierten Geltungsdauer ausführbar sind.
9. Vorrichtung nach Anspruch 1 bis 8, dadurch gekennzeichnet, dass die Freischaltungskomponente einen Freischaltungszähler aufweist, der die Anzahl der Ausführungen einer Funktion pro Freischaltung festlegt.
10. Verfahren zur Freischaltung von Chipkarten, wobei im nichtflüchtigen Speicher der Chipkarte zumindest eine Funktion abgelegt ist, die zu ihrer Ausführung ein Vorliegen einer definierten Zugriffsvoraussetzung erfordert, gekennzeichnet durch folgende Schritte:
    a) Einführen der Chipkarte in ein Gerät zur Aufnahme und Kontaktierung mit der Chipkarte,
    b) Eingeben von Authentisierungsdaten mittels einer Eingabevorrichtung,
    c) Weiterleiten der Authentisierungsdaten zu der Chipkarte
    d) Vergleichen der eingegebenen Authentisierungsdaten mit abgelegten Referenzdaten in der Chipkarte
    e) Ablegen von Daten zum Freischalten der Funktion im nichtflüchtigen Speicher der Chipkarte, deren Vorliegen als Zugriffsvoraussetzung zum Ausführen der Funktion definiert sind falls eine Übereinstimmung von eingegebenen Authentisierungsdaten mit den abgelegten Referenzdaten vorliegt.
11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass das Gerät nach Schritt a) als Taschenchipkartenle-

ser ausgebildet ist.

12. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die Authentisierungsdaten durch einen PIN oder durch biometrische Fingerabdruckwerte repräsentiert werden können.

13. Verfahren nach Anspruch 10 oder 11, dadurch gekennzeichnet, dass die Daten zum Freischalten einer Funktion zusätzlich Daten über Anzahl der Ausführung einer Funktion und/oder Zeitpunkt der Ausführung einer Funktion und/oder Dauer der Ausführung einer Funktion enthalten.

14. Verfahren nach Anspruch 10 bis 11, dadurch gekennzeichnet, dass die Daten für die Anzahl der Ausführung und/oder Zeitpunkt der Ausführung und/oder Dauer der Ausführung der Funktion Teil der Funktion sind.

15. Verfahren nach Anspruch 10 bis 13, dadurch gekennzeichnet, dass das Ablegen der Daten zum Freischalten der auszuführenden Funktion nach Schritt e) in eine Datei im nichtflüchtigen Speicher der Chipkarte erfolgt, wobei diese Datei nur durch das Chipkartenbetriebssystem beschrieben und gelesen werden kann.

16. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die auszuführende Funktion ein digitale Signatur ist.

17. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die auszuführende Funktion ein Lese- oder Schreibkommando ist.

18. Verfahren nach Anspruch 10, enthaltend folgende weitere Schritte:

f) Einführen der Chipkarte in ein Terminal

g) Empfangen eines Anwendungskommandos zur Ausführung einer auf der Chipkarte abgelegten Funktion

h) Überprüfen des Erfordernisses von Freischaltdaten als Zugriffsvoraussetzung zur Ausführung der Funktion

i) Herabsetzen der Anzahl der erlaubten Ausführungen um 1, wenn ein Freischaltungszähler für die auszuführende Funktion vorgesehen ist,

j) Ausführen der Funktion bei Vorliegen der Freischaltdaten.

Hierzu 2 Seite(n) Zeichnungen

Nummer: DE 198 60 177 A1
Int. Cl.[7]: G 06 F 3/08
Offenlegungstag: 6. Juli 2000

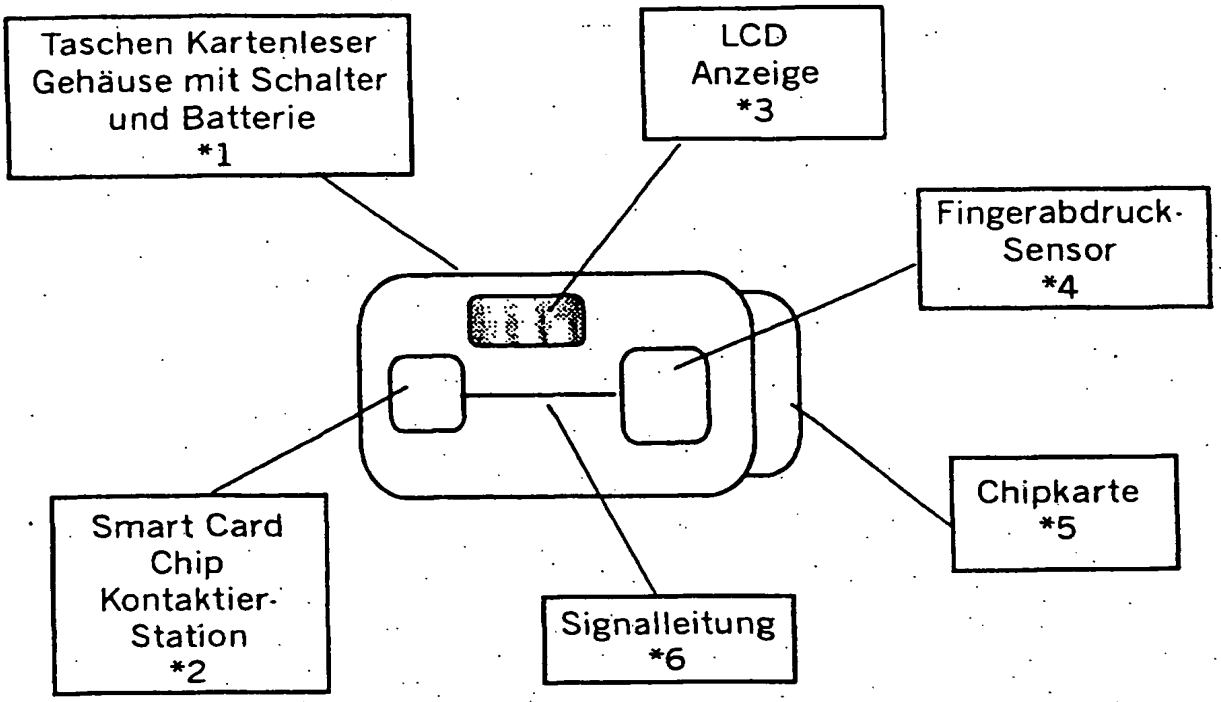


FIG. 1

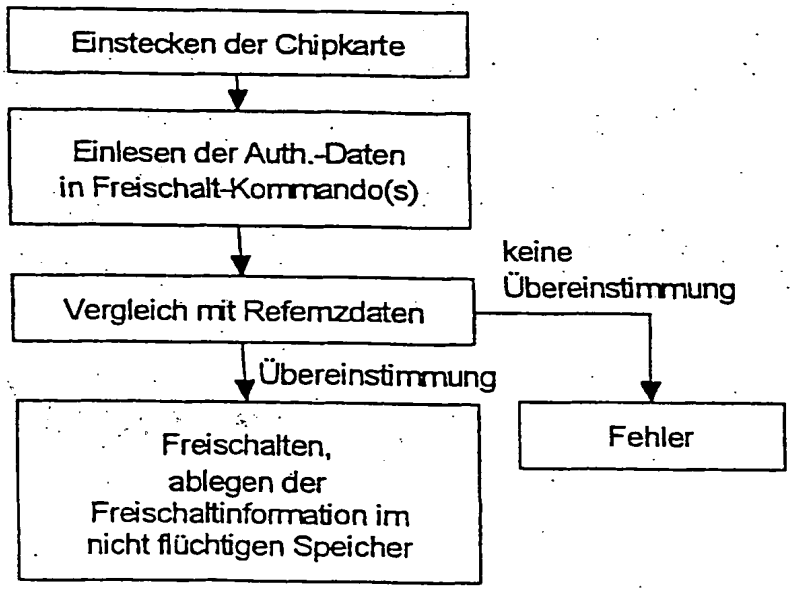


FIG. 2

Nummer: DE 198 60 177 A1
Int. Cl.[7]: G 06 F 3/08
Offenlegungstag: 6. Juli 2000

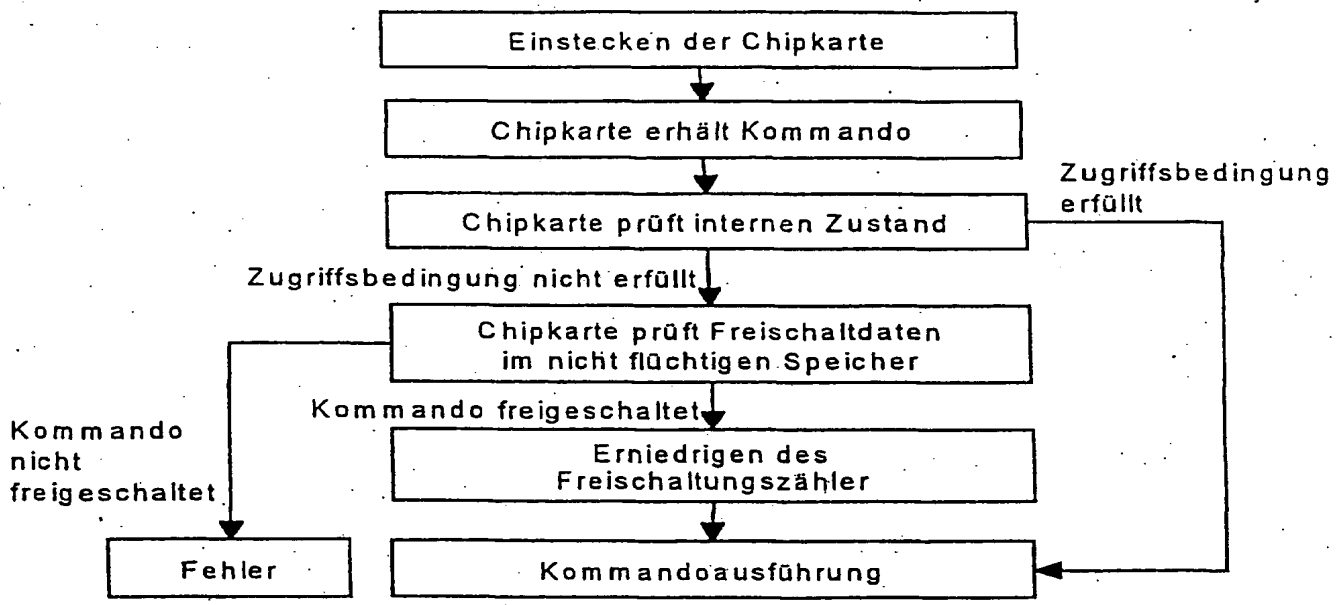


FIG. 3

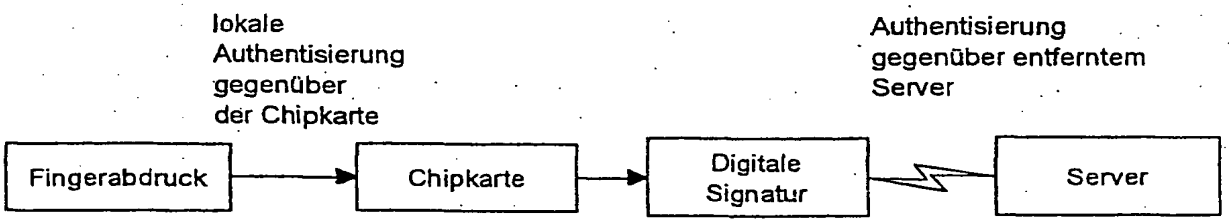


FIG. 4